Declassified in Part - Sanitized Copy Approved for Release 2013/02/28 : CIA-RDP90-00530R000100150001-9

Ltr
Chap 8.

November 4, 1988

STAT

Dear Frank and Elaine:

Enclosed are some words on the subject I promised. There is an organizational issue present in this one -- counterintelligence people are a class of their own. They like to track a condition, network of "leak", focus on catching the foreign perpetrator and documenting a legal and presentable case. The employee violator is not central in their larger context, i.e., "catching" them early and administering preventative medicine is not their bag nor are their files open to HRM people with that more "healing" focus. The Security Officers of the IC fall between the two, i.e., policeman/detective and counterintelligence generator. Files, therefore, are not always shared.

The Panel has not had the charge to address organizational dichotamy, and I feel certain the DCI is sensitive to the arguements on both sides. My paper seeks to stick to our charge, but intrude a little. See you on the 15th.

Warm regards,

John M. Clarke

Enclosure:
as stated

Declassified in Part - Sanitized Copy Approved for Release 2013/02/28 : CIA-RDP90-00530R000100150001-9

Declassified in Part - Sanitized Copy Approved for Release 2013/02/28 : CIA-RDP90-00530R000100150001-9

PERSONNEL SECURITY AND COUNTER INTELLIGENCE OBSERVATIONS

The secrecy systemic to intelligence work, activities, and environments has generated a wide and varying range of personnel security processes in all IC Agencies. These make up a critical part of the larger charge for protecting intelligence sources and methods from foreign espionage -- a charge levied by law on the cryptologic services, DCI, and all IC Agencies.

The NAPA Panel elected to focus on how these processes may impact on recruitment, acquisition, use and separation of employees and to compare results of the practices and experiences of IC Agencies to determine what, if any, change in authority or personnel organizational initiatives might warrant the attention of the Congress.[1/]

The Panel notes that while IC employee security data feed and/or are part of the larger counter intelligence data bank and mission, the organizational compartation of the task to discover foreign espionage activity and networks are quite distinct from internal security processes or personnel programs per se.

No intelligence agency is without major breaches discovered after damage has occured. Many have lost personnel and "secrets" directly to the active and continuing espionage of foreign governments over extended periods before discovery by counter intelligence operatives. This has occurred despite the growing resources provided by Congress for counter intelligence and personnel security processes, to changes in law, and human resource programs designed separately by IC Agencies to nurture commitment and patriotism and to provide employee incentives for long term careers and reward for performance. Clearly penalties for breaching security are well communicated to employees.

The Panel did not explore in depth the degree of employee information exchange among the individual IC Agencies' security nor the potential for added Community coordination on personnel security and counter intelligence relationships therewith. However in pursuit of

---

1/ e.g., These processes range from initial impact on recruitment of personnel security investigation, use of polygraph, etc., to physical security demands of the work place, procedures for handling classified materials and penalties for non-compliance, limitation on behaviorial freedoms of IC Agency personnel, use of secrecy agreements, re-investigations, etc.

Declassified in Part - Sanitized Copy Approved for Release 2013/02/28 : CIA-RDP90-00530R000100150001-9

Declassified in Part - Sanitized Copy Approved for Release 2013/02/28 : CIA-RDP90-00530R000100150001-9

the NAPA study considerable interagency communication on personnel matters took place beyond that previously experienced in the Community. The Panel strongly suggests that employee counter intelligence focus is an area that should be foremost in organizational cooperation and non-parochial in administration.

In context, ~~however~~, the Panel emphasizes support for ongoing IC Agency ~~Programs of~~ proactive attention and research to understanding the significance of a change in employees' attitudal and/or behavior patterns. Vulnerabilities can grow out of employees troubled with "problems". They often manifest themselves in identifiable change in the attitudes, life style, and behavior that can telegraph early warning of possible susceptibility to influence by foreign intelligence operatives or even to vindictiveness toward their intelligence employer. Fellow employees, friends, and supervisors are likely to be first to directly sense or observe such changes. Understandably, the experience is that IC employees' basic trust in one another, preoccupation with work tasks, the cultural pattern of minding one's own business, respect for privacy, the general tendency of individual distancing from "tattle tales", and even disinterest all mitigate against such indicational data flowing from employee sources for use in "defensive" counseling. Regular informal employee conferences and evaluations can help discover such indicators and trigger machinery for counseling, but these take time away from job tasks for which people are rewarded. The sensitivity of supervisors to such indicators and holding them accountable for early warning are critical ingredients.

The Panel finds that all IC Agencies HRM programs have adequate authority and resources to pursue this task aggressively. The Panel particularly endorses and commends current efforts at strong and regular "risk assessments" for personnel who may leave disgruntled. The Panel endorses the use of all flexible HRM means available to prevent and avoid such circumstances. The Panel urges risk assessments of potential employee disaffection be increasingly communicated to other IC Agencies who may be impacted.

Declassified in Part - Sanitized Copy Approved for Release 2013/02/28 : CIA-RDP90-00530R000100150001-9